Title 22, Division 14
California Office of Health Information Integrity

Table of Contents

Division 14 California Office of Health Information Integrity

Chapter 1 HIE Demonstration Projects

§126010 Applicability of Regulations

(a) The regulations in this chapter apply to Demonstration Project Participants and Health Information Exchange Service Participants, as defined in California Health and Safety Code §130276.

(b) Effective dates. The regulations in this chapter are effective on **[insert the date filed with secretary of state].**

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: California Health and Safety Code §§§§ 130276, 130277,130278, 130282.

§126020 Definitions

(a) "Access" means the ability or the means necessary to read, write, modify, or communicate data or information or otherwise use any health information.

(b) "Applicant" means an entity that submits an application to CalOHII for approval as a Demonstration Project.

(c) "Business Associate" means:

(1) With respect to a health care provider, an entity on behalf of such health care provider, but other than in the capacity of a member of the workforce of such health care provider who:

(A) Performs, or assists in the performance of a function or activity involving the use or disclosure of identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or

(B) Provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such health care provider, where the provision of the service involves the disclosure of individual health information from such health care provider or from another business associate of such health care provider, to the person.

(2) A health care provider may be a business associate of another health care provider.

(d) "Business Associate Agreement"

A contract or other arrangement between a health care provider and its business associate, required by HIPAA (45 C.F.R. §164.308(b)), that specifies the permitted uses and disclosures of individual health information, requires the use of appropriate safeguards to prevent the use or disclosure of the individual health information other than the permitted purposes specified in the agreement, and details the scope of any other responsibilities.

(e) "CalOHII" means the California Office of Health Information Integrity.

(f) "De-identified health information" means health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Compliance with federal standards for de-identification of health information, as codified 45 C.F.R. § 164.514, shall be deemed adequate for de-identified health information.

(g) "Direct exchange" means the electronic exchange or access to of health information without the use of a health information organization:

(1) Through a direct connection between the electronic health record systems of health care providers; or

(2) From a health care provider or entity to another health care provider or entity utilizing national or state standards, services, and policies including but not limited to the standards, services and policies of the Direct Project of the National Health Information Network.

(h) "Electronic Health Record (EHR)" means an electronic record of health information about an individual and that can be created, managed, and consulted by authorized clinicians and staff.

(i) "Entity" means a person, corporation, association, partnership or other legal entity, other than an individual or the individual's personal representative in possession of health information pertaining to the individual.

(j) "Health Care Provider" means a person or entity that is a health care provider under 45 C.F.R. § 160.103, or is a provider of health care under California Civil Code § 56.05(j).

(k) "Health Information" means any information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, health care clearing house, personal health record, health information organization, or any other entity; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual

(l) "Health Information Exchange" (HIE) means the electronic movement or access to health information.

(m) "Health Information Organization" (HIO) means an entity that oversees and governs the exchange of or access to health information.

(n) "Individual" means the person who is the subject of health information.

(o) "Individual Health Information" (IHI) means information about an individual that alone or in conjunction with other reasonably available information includes or relates to:
(1) Demographic information,
(2) The past, present, or future physical or mental health or condition of the individual
(3) The provision of health care to an individual, or
(4) The past, present, or future payment for the provision of health care to an individual.

(p) "Participant" means a demonstration project Participant.

q) "Public Health" This term refers to public health authorities whose public health programs promote, maintain, and conserve the public's health by providing health services to individuals and/or by conducting research, investigations, examinations, training, and demonstrations. This definition is consistent with state and federal definitions of public health programs and as the term is used in the meaningful use incentive program.

(r) "Trading Partner" means an entity that has a Trading Partner Agreement with an Applicant or Participant for the exchange of information in electronic transactions.

(s) "Trading Partner Agreement" means an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

(t) "Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers related to a patient; or the referral of a patient for health care from one health care provider to another.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: California Civil Code§§ 56.05, 56.06; Health and Safety Code §§ 130200, 130201, 130276, 130277, 130278; 45 C.F.R. §§160.103, 164.304,164.501.

§126030 California Health Information Exchange Practices Principles

(a.) Participants shall adhere to the following principles of fair information practices:

(1) Openness – There should be a general policy of openness among entities that participate in electronic health information exchange about developments, practices, and policies with respect to individual health information.

(2) Individual Health Information Quality – Health information shall be relevant, accurate, complete, and kept up-to-date.

(3) Individual Participation – Individuals or their personal representatives have the right to:

(A) Ascertain the person responsible for individual health information for an entity, obtain confirmation of whether the entity has specific individual health information relating to the individual, and obtain its location.

(B) Receive their individual health information in a reasonable time and manner, at a reasonable charge, and in a format that is generally accessible by individuals.

(C) Challenge the accuracy of their individual health information and, if successful, to have the individual health information corrected, completed, or amended.

(D) Control the access, use, or disclosure of their individual health information, unless otherwise specified by law or regulation.

(4) Collection Limitation – There shall be limits to the collection of individual health information. Individual health information shall be obtained by lawful and fair means. Where appropriate, it shall be obtained with the knowledge or consent of the individual or their personal representative. The specific purposes for which individual health information is collected shall be specified not later than at the time of collection.

(5) Individual Health Information Limitation – Use and disclosure of individual health information shall be limited to the specified purpose. Certain use and disclosure shall require consent.

(6) Purpose Limitation - Individual health information shall be relevant to the purpose for which it is to be used and, limited to the minimum information necessary for the specified purpose. The subsequent use shall be limited to the specified purpose.

(7) De-Identified Information – De-identified individual health information shall not be re-identified unless specified in law. If de-identified individual health information is re-identified, it shall be subject to these principles. De-identified individual health information shall not be disclosed if there is a reasonable basis to believe that the information can be used to identify an individual.

(8) Security Safeguards – Individual health information should be protected by appropriate security safeguards against such risks as loss or destruction, unauthorized access, use, modification or disclosure of data.

(9) Accountability – An entity shall comply with laws, regulations, standards and organizational policies for the protection, retention and destruction of individual health information. Any person who has access to individual health information shall comply with those provisions.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126040 Transparency and Complaint Process

(a) Prior to the approval of any demonstration project, the Applicant must provide CalOHII with copies of:
(1) The Applicant's Notice of Privacy Practices
(2) All of the Applicant's Data Use Agreement(s) and a list of the entities included in the data use agreement
(3) A description of the Applicant's complaint mechanism required by §126040(d), including any documentation or patient educational materials related to the complaint process.

(b) Once a demonstration project is approved, but prior to the start of the demonstration project, within a specified time frame negotiated with and approved by CalOHII, the Participant must provide

(3) A list of all of the Participant's current business associates and trading partners, with their contact information and a general description of the service(s) provided, including the data shared, the purpose, and whether further dissemination of the data is allowed, regardless of whether the information is de-identified. This requirement may be modified to reflect only those business associates and trading partners with access to the individual health information exchanged through the demonstration project.
(A) If a new business associate or trading partner is added after the start of the project, or a business associate agreement or trading partner agreement is modified, the Participant must provide CalOHII with an updated list within 20 business days of the commencement of the business associate agreement or data exchange partner agreement or the provision of services, whichever is earlier.
(B) In CalOHII's discretion, CalOHII may require copies of the Participant's business associate agreements and trading partner agreements be provided to CalOHII. The Participant shall provide copies within five working days from the receipt of written request from CalOHII.

(c) All unauthorized disclosures or access of individual health information shall be reported to CalOHII within five business days. A report to CalOHII under this provision

does not relieve the Participant from any requirement under any local, state, or federal law.

(d) Participants must ensure there is a mechanism to receive and respond to patient complaints.
  (1) Complaints associated with the demonstration project shall be reported and forwarded to CalOHII within 20 business days from the date the complaint is made.
  (2) The Participant's response to any complaint regarding the demonstration project shall be forwarded to CalOHII within ten business days of the response.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126050 Health Information Exchange Permitted Purposes

(a) Permitted purposes. Individual health information exchanged or accessed through an HIO or a direct exchange shall be limited to:
  (1) Treatment
  (2) Reporting to Public Health Officials for immunizations, bio-surveillance and mandated reporting.
  (3) Quality reporting for meaningful use to Centers for Medicare and Medicaid Services and the California Department of Health Care Services.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126060 Notice and Consent; exceptions

(a) Notice
  (1) Prior to requesting an individual or the individual's personal representative to permit the electronic exchange of health information, an entity shall provide notice to the individual or the individual's personal representative, which at a minimum shall contain statements describing:
    (A) Electronic exchange of health information
    (B) Uses of data exchanged using electronic health information exchange
    (C) Benefits and risks associated with electronic health information exchange, including the exchange of sensitive health information, such as HIV status, mental health records, reproductive health records, drug and alcohol treatment records, and genetic information which could be inferred or embedded in information that is made available in the exchange.
    (D) Consent requirements for electronic health information exchange
    (E) Specific exceptions to the consent requirements for electronic health information exchange for mandated public health reporting

(F) Specific exceptions to the consent requirements for electronic health information exchange in emergency situations
(G) Process for revoking consent, including a contact name, phone number, email address, and website
(H) When the revocation of consent is effective

(b) Affirmative Consent
(1) Before an individual's individual health information is electronically exchanged, an entity shall obtain written affirmative consent documenting the individual's or the individual's personal representative's choice to electronically exchange the individual's individual health information.

(2) Obtaining affirmative consent documenting the individual's or the individual's personal representative's choice to electronically exchange their individual health information does not relieve the entity from obtaining legally required authorizations to disclose health information.

(3) Emergency situations
(A) A licensed health care provider may access an individuals' individual health information when:
1. The individual requires emergent care;
2. The individual or the individual's personal representative is incapable of consenting;
3. The individual or the individual's personal representative has not explicitly denied or withdrawn consent on a previous occasion; and
4. It is in the best interest of the individual, as determined by the treating health care provider.

(4) Mandated public health reporting. Affirmative consent is not required for mandated public health reporting disclosures.

(c) Revocation of consent
(1) An individual or the individual's personal representative may revoke their previously granted consent to the electronic exchange of health information by contacting the designated contact person or entity as described in the Notice required by section (a).
(2) After the effective date of the revocation of consent, the demonstration project Participant or health information exchange service Participant shall not allow the individual's individual health information to be electronically exchanged unless and until the individual or the individual's personal representative reinstates consent.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126070 Security Requirements - General

(a) Scope – These security policies shall apply to individual health information in any form whether accessed, licensed, stored, transmitted or maintained. For individual health information that has not been accessed, transmitted, or received on or after the effective date of these policies, the requirements under Sections 126076(d) and 126078 do not apply.

(b) General Requirements. Participants must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic individual health information (IHI) the entity creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under California law.

(4) Ensure compliance with these requirements by the entity's workforce and any entity that receives or uses IHI on the participant's behalf.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 56.13 1798.21, 1798.81.5; Health and Safety Code §§ 130200, 130277, 130279; 45 C.F.R. §§ 164.302, 164.306(a)

§126072 Security Requirements – Administrative

A demonstration project participant must do the following:

(a) Information Security (Organization & Responsibility). An entity shall identify the entity's primary security official who is responsible for implementation and compliance to these requirements. Such official shall be identified in such a way that anyone who might have a security issue or concern may contact that person.

(1) Responsibility & Coordination of Information Security Assets. An entity shall account for information security assets and designate the asset owner(s). Appropriate security controls shall be assigned for each class or group of information security assets. Implementation of specific controls may be delegated by the owner as appropriate. The owner remains responsible for the proper protection of the assets in all cases where delegation occurs.

(2) Information Security Policy Approvals & Management. An entity shall comply with the following:

(A) In deciding which security measures to use, an entity shall, at a minimum, take into account the following factors:

(i) The size, complexity, and capabilities of the entity.

(ii) The entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs/benefits of security measures.

(iv) The probability and criticality of potential risks to individual health information.

(B) This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this chapter

(3) Applications Inventory. An entity shall identify all operating, database, and application assets (e.g. application software, system software, development tools) that support the exchange and processing of individual health information and document the importance of these assets. An application inventory shall include all information necessary in order to recover from a disaster or other business interruption, such as, but not limited to, application logging, type of asset, format, location, backup information, license information, and business value

(4) Isolating Health Care Clearinghouse Functions. If a health care transaction clearinghouse is part of a larger entity, the clearinghouse segment shall protect and isolate individual health information of the clearinghouse from unauthorized access by the larger organization.

(b) Risk Management Program. An entity shall develop and implement a risk management program that enables the entity to assess and reduce risk to an acceptable level.

(1) Risk Assessment. An entity shall periodically conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of individual health information held, created, processed, transmitted or received by an entity.

(2) Risk Management & Mitigation. An entity shall implement security measures sufficient to reduce risks and vulnerabilities to:

(A) Protect the confidentiality, integrity, and availability of all individual health information the entity creates, receives, maintains, or transmits.

(B) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(C) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under this chapter.

(D) Take steps to ensure compliance with these requirements by its workforce.

(c) Workforce Security Management. With regard to managing sensitive data, an entity shall ensure that all members of its workforce have appropriate access to individual health information and prevent workforce members from obtaining unauthorized access to individual health information.

(1) Workforce Supervision. An entity shall establish a process for authorizing and managing access provisioning and controls for workforce members. An entity shall supervise workforce members. At minimum, an entity shall supervise workforce members by employing the following guiding principles:

(A) Least access privileges necessary

(B) Default to no access

(C) Review and adjust privilege, if needed, upon change of job duties or other changes that impact the need for access

(D) Promptly remove access to individual health information when access is no longer required

(E) Periodic review of workforce access privileges

(2) Workforce Sanctions & Accountability. An entity shall apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the entity.

(3) Permitted Use of Equipment. An entity shall specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation, including but not limited to, mobile computing devices that can access individual health information.

(d) Compliance Testing, Audit & Monitoring. An entity shall take steps to ensure compliance of their systems with these security requirements. The security of information systems shall be regularly reviewed. Such reviews shall be performed against these provisions:

(1) Non-compliance found. If any non-compliance is found as a result of the review, managers shall, at a minimum:

(A) Determine the causes of the non-compliance

(B) Remediate issues found to cause non-compliance, or management shall respond indicating why this risk was accepted or not applicable

(C) Evaluate the effectiveness of the corrective action, post-implementation.

(D) Perform appropriate breach reporting, as required by HIPAA, California law and contractual requirements.

(2) Activity Review & Monitoring (Logs). An entity shall regularly review records of activity and monitor information systems that contain IHI. Review information security controls (such as audit logs, access reports, and security incident tracking reports) for indications of control failure or exploitation of information systems. An entity shall take actions to remediate, as appropriate.

(3) Evaluation of Policy and Technical Compliance. An entity shall perform and document a technical and non-technical evaluation on an iterative basis that demonstrates due diligence and an active evaluation program. Iterative reviews should be performed whenever environmental, operational, or technical changes occur that may introduce security vulnerabilities.

(e) Security Incident Management Response, & Documentation. An entity shall address security incidents. An entity shall identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security

incidents that are known to the entity; and document security incidents and their outcomes. An entity shall take measures necessary to determine the scope of the breach and correct offending deficiencies in security controls to prevent a recurrence of the breach of the information system.

(f) Frequency of Actions. Activities required by this chapter shall be performed at a frequency determined by an entity based on knowledge of activities and/or changes within the organization, or as required by other legal or contractual obligations.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.20,1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. §§ 164.302, 164.306, 164.308,164.310(b)

§126074 Security Requirements – Contingency Planning

(a) Contingency Planning. An entity shall document a comprehensive business continuity plan and recovery strategies including elements related to people, processes, environment, incident management, and coordination with emergency response, crisis communications, and individual health information data. Such a plan should include a listing of identified risks and mitigation or acceptance statements for each risk. (See: Section 126072(b) Risk Management Program). Participants implementing operations subject to these requirements are responsible for understanding and being compliant with applicable federal, state and local legislation and regulatory requirements related to business continuity planning.

(1) Business Impact Analysis. An entity shall document a Business Impact Analysis that identifies any vulnerability and develop strategies for minimizing risk. The Analysis should describe the potential risks specific to the entity and all critical business components. The BIA shall include, but is not limited to:

(A) Applications & Data Criticality Analysis

(B) Change Management

(2) Recovery Strategies. An entity shall document strategies for business recovery from a serious disruptive event. The recovery strategies should define procedures to be followed to achieve a structured and coherent recovery process. The entity shall review any pre-defined procedures in the event of an actual situation arising following a disruptive event and modify these procedures as appropriate. Defined procedures should include, but are not limited to:

(A) Incident Management

(B) Emergency Response

(C) Crisis Communications

(D) Disaster Recovery Plan, to include:

(i) Technical Recovery Plans

(ii) Facilities

(iii) Business Recovery Plans

(3) Business Continuity Plan. An entity shall implement a Business Continuity Plan that details procedures and processes for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages, or makes inaccessible, systems that contain individual health information. Consideration should be given to multi-system approach, inter-disciplines, all locations where IHI resides, and all business process boundaries (interface points). The Continuity Plan shall include, but is not limited to:

(1) Business Impact Analysis (BIA)

(2) Recovery Strategies

(3) Testing and Revision of the Continuity Plan

(4) Testing & Revision of Contingency Plan. An entity shall create and maintain applications/systems to protect the integrity and availability of individual health information. An entity shall periodically test and revise their contingency plan.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.21, 1798.81.5; Health and Safety Code §§1280.15, 130200, 130277, 130279; 45 C.F.R. § 164.308(a)(7)

§126076 Security Requirements – Facility & Equipment Controls

(a) Facility Access Controls. An entity shall limit physical access to its information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

(1) Physical Access Management. An entity shall safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft, including procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. An entity shall document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks)

(2) Communications and Operations Management. An entity shall assign responsibilities for the management and operation of all information processing facilities that handle individual health information. An entity shall establish formal exchange policies, procedures, and controls to protect the exchange of information through the use of all types of communication facilities.

(b) Device & Media Controls. An entity shall control, administer and maintain a record of the consignment of hardware and electronic media that contain individual health information and any person responsible therefore and maintain the inventory of such assets.

(1) Mobile Electronic Device Controls. An entity shall limit and protect the storage of Individual Health Information (IHI) on mobile electronic computing devices and passive storage media. An entity shall have a policy directing all workforce members, using any non-managed (user-owned) devices or media, to adhere to the user's entity requirements identified in this chapter. Storage of IHI on mobile computing devices and passive storage media is prohibited unless the devices or IHI:

(A) Are physically secured in accordance with this Chapter

(B) Are encrypted where indicated by risk assessment, using minimum encryption standards identified in this Chapter

(C) Legacy medical devices may require alternative controls in lieu of standard controls as allowed by device manufacturers, such deviations from standard controls shall be documented

(2) Workstation & Security Equipment Controls. An entity shall implement physical and/or technical safeguards for all workstations that access individual health information, to restrict access to authorized users.

(3) Unsecured IHI Loss Prevention. An entity shall take reasonable steps to prevent the unauthorized removal or transmission of individual health information, including but not limited to, data leakage, laptop or flash drive loss, etc.

(4) Reuse of Media. An entity shall implement procedures for removal of individual health information from electronic media before the media is made available for re-use.

(5) Disposal of Media. An entity shall utilize a method that best meets the entity's business practices and protects the security of individual health information for final disposition of individual health information, hardware, and/or electronic media on which the individual health information is stored.

(A) The media on which the PHI is stored or recorded shall be destroyed in one of the following ways:

(i) Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or reconstructed. Redaction is specifically excluded as a means of data destruction.

(ii) Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800–88, Guidelines for Media Sanitization.

(c) Technical Controls. An entity shall protect individual health information in information systems as specified in these provisions.

(1) Login Monitoring. An entity shall monitor log-in attempts, reporting discrepancies, and take actions to remediate, as appropriate.

(2) OS & DB Hardening / Patch Management. As appropriate, an entity shall comply with the following for the protection of individual health information:

(A) Apply patches or use other appropriate mechanisms (e.g., update the operating system (OS) and databases) on a timely basis

(B) Harden and configure the OS and databases to address security vulnerabilities

(C) Install and configure necessary security controls

(D) Regularly test the security of the OS and databases to ensure that the previous steps address known security issues

(3) Malicious Code Protection. An entity shall take appropriate steps to protect against malicious software. In addition, an entity shall incorporate a mechanism to detect, mitigate the effect of malicious software, and immediately report malicious software to the primary security official or designee for response if necessary.

(4) Email & Messaging Security. An entity shall safeguard electronic mail and messaging containing individual health information in its possession.

(5) Audit Controls. An entity shall implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use individual health information.

(d) Network Security Management. An entity shall protect the networks and infrastructures that maintain or transmit individual health information.

(1) Perimeter Controls and Management. An entity shall identify and include, or reference, security features, service levels, and management requirements of all network services in any network services agreement, whether these services are provided in-house or outsourced. Network services include the provision of connections, private network services, and value added networks and managed network security solutions such as firewalls and a system to detect intrusion.

(2) Intrusion Detection. An entity shall implement an internal system to detect intrusion attempts. The entity shall document and report successful intrusions to the primary security official or designee for response.

(3) Consistent Time. An entity shall take steps to ensure clocks of all relevant information processing systems within an organization are synchronized using an accurate reference time source using the Network Time Protocol (NTP).

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§ 1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. § 164.306(a), 164.308(a)(5),164.310, 164.312.

§126078 Security Requirements – Access Controls

(a) Access Controls. An entity shall utilize identity management, authentication, and authorization mechanisms to ensure that only authorized users have access to information systems.

(1) Identity Management (Internal). An entity shall establish policies and procedures to verify the identity of workforce members who will access the entity's systems. An entity shall, at a minimum:

(A) Verify that the individual is the one claimed by examination of various forms of state-issued picture identifications such as a driver's license or ID card, professional licenses in good standing from state or national certification boards, and other forms of identification issued by reliable bodies. The number and extent of such verification will be commensurate with the user's responsibilities and consistent with privileges they will be given (authorizations).

(B) Issue a user identifier and an identity certificate and/or token (password, hard token, soft cryptographic token or one-time password device tokens, etc.), to the verified person, as appropriate to their level of authorization.

(C) Be responsible for any health data access rights assigned to the authorized person based on their qualifications and role.

(D) Manage all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services.

(2) Single Entity Authentication (Non-Federated). An entity shall authenticate each authorized user's identity prior to providing access to individual health information.

(A) An entity shall assign a unique name and/or number for identifying and tracking user identity and implement procedures to verify that a person or entity seeking access to individual health information is the one claimed.

(B) An entity shall authenticate each user to the level of authorized access that complies with the entity's level of trust agreement with the external exchange entity.

(C) An entity shall authenticate users attempting to access individually identifiable health information from an unsecured location or device, shall require NIST Level 3 authentication in which the data requester must establish two factors of authentication. [See NIST SP 800-63 Rev-1]

(3) Authentication Across Multiple Participants (Federated).

(A) If an entity is participating in a trust network HIE:

(i) The trust network shall manage entity authentication for those participating on the trust network, and

(ii) An entity shall manage user authentication only for those participants participating on the trust network.

(B) If the user authentication process is across multiple systems or entities:

(i) An entity shall implement the agreed upon authentication process among the participants in the trust network.

(C) An entity participating in the trust network shall implement a trust agreement.

(D) The entity shall adopt an authentication solution that incorporates the authorization requirement of this chapter. l.

(4) Authorization & Access Control.

(A) An entity shall use the following access control attributes to determine if a user is authorized to access requested information in a way that corresponds to, and is compliant with, the data use agreements governing such access and as it aligns with state requirements:

(i) Data Source;

(ii) Entity of Requestor;

(iii) Role of Requestor;

(iv) Use of Data;

(v) Sensitivity of Data;

(vi) Consent Directives of the Data Subject

(B) An entity that acts as a data requestor shall execute the authorization process at the location agreed upon in the data use agreements governing that exchange. The data requestor shall pass the authentication and authorization to the data supplier as a single message if so designated by the data use agreement.

(5) Password Management. Where an entity uses password authentication, it shall require passwords to be created, changed periodically, safeguarded, and of sufficient length and complexity to protect individual health information.

(A) Note: As applicable, passwords shall be used for all mobile computing devices and passive storage media that contain IHI.

(6) Session Controls. An entity shall implement procedures and technical controls to protect against the unauthorized access to individual health information via workstations, which can include, but are not limited to:

(A) Setting session timeout due to inactivity

(B) Password protection for locking screens

(C) Lockout based on unsuccessful logon attempts

(D) Turn on access (security event) logs and regularly review

(E) Limit physical access to workstations

(b) Data Assurance. An entity shall protect individual health information from unauthorized alteration or destruction. An entity shall implement technical security

measures to guard against unauthorized access to, or modification of, individual health information that is being transmitted over an electronic communications network.

(1) Encryption & Cryptographic Controls. An entity shall utilize encryption to the level appropriate to the data being protected, and where appropriate, to protect individual health information. Participants shall utilize the NIST Cryptographic Module Validation Program (CMVP) as the authoritative source of which products, modules, and modes are approved for use by NIST for Federal information Processing. This list, or its successor, should be periodically reviewed for updated information as part of each organization's internal best practices.

(2) Integrity Controls. An entity shall implement security measures to safeguard electronically transmitted individual health information from being modified without detection until disposed. This includes implementation of electronic mechanisms to corroborate that individual health information has not been altered or destroyed in an unauthorized manner.

Authority: California Health and Safety Code §§ 130277, 130278.

Reference: California Civil Code§§1798.21, 1798.81.5; Health and Safety Code §§ 1280.15, 130200, 130277, 130279; 45 C.F.R. §§ 164.308(a)(4) & (a)(5),164.312

§126080 Requests to Waive Requirements

(a) An Applicant may request CalOHII waive a requirement of sections 126050, 126060, 126070, 126072, 126074, 126076, and 126078 for the Applicant's demonstration project if the Applicant is currently unable to comply with the requirement. All requests for waivers must be submitted to CalOHII in writing, and include:
  (1) The reason for waiver request
  (2) All supporting documentation, such as:
    (A) If the reason is related to implementation delays, state the timeframe in which the requirement will be implemented
    (B) A description of, and copies of alternate privacy and security provisions that would provide similarly adequate compliance with the California Information Exchange Practices Principles.

(b) Granting waivers of requirements is in the sole discretion of the Director of CalOHII.

(c) The Director of CalOHII shall document in writing each grant of a waiver of a requirement within a reasonable time frame.

(1) Unless a waiver is expressly granted in writing, Participants must comply with all requirements of these regulations.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Health and Safety Code §§ 130200, 130277, 130279.

§126090 Health Information Exchange Demonstration Projects Oversight

(a) CalOHII may audit Participants for compliance with these regulations at any time. An audit may include, but is not limited to inspection of:
  (1) Privacy and security policies and procedures
  (2) Training documentation
  (3) Business associate agreements
  (4) Data exchange partner agreements
  (5) Operations of the demonstration project

(b) The Participant must provide CalOHII with any and all requested documentation pertaining to 126090(a) within 10 business days.

(c) CalOHII may conduct a site visit to observe operations of the demonstration project and compliance with these regulations.

(d) If CalOHII determines a Participant is not in compliance with these regulations, a notice of non-compliance will be issued.

(1) A Participant receiving a notice of non-compliance shall submit a plan of correction to CalOHII within 10 business days of the receipt of the notice of non-compliance

(A) If CalOHII determines the plan of correction does not adequately address the identified instances of non-compliance, it may reject the plan of correction and request a Participant to modify the plan of correction and resubmit within 5 business days.

(2) CalOHII may terminate a demonstration project if:

(A) CalOHII determines a Participant has not adequately addressed identified areas of non-compliance; or

(B) If the Participant has not complied with an accepted plan of correction; or

(C) If the non-compliance with the regulations is so egregious as to imminently threaten the security or privacy of the health information held by the Participant.

Authority: California Health and Safety Code §§ 130277, 130278.
Reference: Government Code§ 11180 et seq.; Health and Safety Code §§ 130200, 130277, 130279.